בנק ישראל

מזכירות הוועדה המייעצת

פרוטוקול מישיבת הוועדה המייעצת להוראות הממונה על שיתוף בנתוני אשראי (2/2018)

שהתקיימה בתאריך 12.2.2018 במשרדי בנק ישראל בתל אביב

נוכחים מקרב חברי הוועדה: עודד שריג - יו"ר הוועדה המייעצת
רני נויבואר - סגן יו"ר
אוריאל לדרברג
אלמה כהן
כפיר בטט
כרמי אור
לימור שמרלינג מגזניק
רונן הורוביץ

נוכחים מקרב עובדי הבנק: צוריאל תמם, הממונה על שיתוף בנתוני אשראי (להלן הממונה)
שירלי אבנר, המחלקה המשפטית
קרן גבאי, המחלקה המשפטית
עובדי הממונה: אורלי הר ציון
אירית זמיר
דורית לואיס, מזכירת הוועדה המייעצת
ויסאם נאטור

הדיון:

הנושא בסדר היום: הוראה ללשכות - ניהול המידע והגתו

הממונה: מבקש לברך על הצטרפותו של כפיר בטט כחבר בוועדה ונציג האוצר. מר בטט היה מעורב בתהליך חקיקת חוק נתוני אשראי.

יו"ר הוועדה: מצטרף לברכות. מבקש שאם יש למישהו מחברי הוועדה ניגוד עניינים לגבי הנושאים הנדונים היום הוא יצהיר על כך. מבין שאין ניגודי עניינים, ולכן ניתן להתחיל בדיון.

הממונה: תהליך ההסדרה מול הלשכות החל לפני כשנה במטרה לייצר ללשכות הפוטנציאליות וודאות רגולטורית. במסגרת התהליך החברות שהגישו בקשה לרישיון לשכה, מסרו לנו את הערותיהן להוראות, שקיבלנו היכן שיכולנו, ומה שמועלה היום לדיון הוא הנוסח המעודכן.

יו"ר הוועדה: ההתרשמות שלי שהושקעה הרבה עבודה בהכנת ההוראה והתוצר טוב. אני מבין שרוב הסיכון של אבטחת המידע נמצא בבנק ישראל שמנהל את המאגר ולכן בנק ישראל יצטרך לעמוד לפחות בסטנדרטים שנקבעו בהוראת "ניהול המידע והגנתו".

מזכירת הוועדה: אכן. הבסיס החוקי לכתיבת ההוראה הינו הסעיפים בחוק נתוני אשראי, תשע"ו-2016 (להלן החוק) המתייחסים לדרישות הרישוי מלשכות וליכולתו של הממונה

לקבוע הוראות ללשכות לשם הגנה על פרטיות הלקוחות ואבטחת המידע. בכתיבת ההוראה התבססנו בין היתר על הוראת ניהול בנקאי תקין מס' 357 - "ניהול טכנולוגיות המידע" החלה על תאגידים בנקאיים, ועל תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017. תהליך העבודה על ההוראה כלל עבודה משותפת של עובדי הממונה ועובדי המאגר (הסתכלות עסקית וטכנולוגית) שארך מעל שנה, דיאלוג כאמור עם הלשכות הפוטנציאליות וכן ניהול דיאלוג עם הרשות הלאומית להגנת הסייבר. להערכתנו, נוסח ההוראה משקף נהלים מיטביים הנהוגים בארגונים המנהלים מאגרי מידע רגיש, תוך שהוא מותאם להערכת הסיכונים שבפעילות של לשכת אשראי, שתפעל במודל עצמאי. הערכת הסיכון של אבטחת מידע הינה מתונה יחסית, שכן המידע עובר ללשכה רק בהסכמת לקוח, לא מדובר במידע טרנזקציוני אלא רק יתרות, לשכה תמחק את המידע לאחר תום השימוש בו והגישה למאגר הלא מזוהה תהיה רק במודל אירוח, תחת מערך אבטחת מידע חזק באחריות בנק ישראל.

חברת הוועדה: האם תקנות הגנת הפרטיות הם הרובד הבסיסי?

נציגת המחלקה המשפטית: כן. מעבר לזה קיים רובד נוסף של כללי הנגידה מכוח סעיף 60(ג) לחוק נתוני אשראי - כללי חוק נתוני אשראי (אבטחת מידע) שנמצאים בשלבי גיבוש ביחד עם הרשות להגנת הפרטיות במשרד המשפטים.

חברת הוועדה: לגבי כללי הנגידה מכוח סעיף 60(ג) מציינת כי מזה תקופה לא הועבר נוסח מעודכן.

הממונה: התקנות והכללים האמורים הם המינימום, ומעבר לזה הרגולציה שתחול על לשכות אשראי (כמפורט בהוראה) הינה יותר רחבה. לגבי לשכת מידע על עוסקים - יחולו רק תקנות הגנת הפרטיות, שכן אין שינוי בהתנהלות שלהן במעבר לחוק החדש. לגבי כללי הנגידה מכוח סעיף 60(ג), הדיונים מול הספק נמשכו ומייד כשנסיימם נעביר עותק מעודכן לרשות להגנת הפרטיות.

יו"ר הוועדה: האם יש לחברים הערות כלליות להוראה? לגבי סעיף 9 - פטור ללשכה - האם הפטור הוא תמידי או קצוב בזמן? מציע להוסיף: "ורשאי הממונה לקבוע כי הפטור יינתן לתקופה קצובה כפי שתיקבע על ידו".

הממונה: מקובל. מציין כי קיבלנו החלטה כי הלשכות ימחקו את נתוני האשראי שיקבלו מהמאגר תוך מספר ימים.

חברת הוועדה: מה לגבי דוחות האשראי שמקבל נותן האשראי מהלשכה?

הממונה: טרם הוחלט סופית, אבל הכיוון המסתמן הוא שנטיל על נותן האשראי את החובה לשמור את דוח האשראי ולמסור אותו ללקוח לפי בקשתו, כמפורט בחוק.

חברת הוועדה: אם הלשכה לא שומרת את נתוני האשראי, איך היא תוכל לעשות בדיקת תיקוף למודל הדירוג? האם בנק ישראל שומר את המידע שהלשכה תעביר לנותן האשראי?

הממונה: הלשכה תוכל לעשות את בדיקת התיקוף על המאגר הלא מזוהה, שיונגש לה בתדירות חודשית, שכן היא תוכל לראות אם אותו לקוח שמופיע במאגר הלא מזוהה אכן נכנס לכשל (הלשכות מקבלות נתונים עם עומק היסטורי של 5 שנים).

בנק ישראל לא שומר את דוחות האשראי שהלשכה מעבירה לנותן האשראי.

נציגת המחלקה המשפטית: בנק ישראל לא שומר את דוחות האשראי, אבל בהתאם לסעיף 23(ב) לחוק שומר את הנתונים שנמסרו בעבר ללשכות, והן רשאיות לקבל את הנתונים הללו אם הם דרושים להן לצורך הליך משפטי בינם לבין הלקוח.

חבר הוועדה: מציין כי לדעתו ההוראה מאוד דומה להוראת ניהול בנקאי תקין מס' 357 החלה על תאגידים בנקאיים, וכי היא הוראה כבדה שלא לצורך. אינו מבין מדוע לשכה צריכה מנגנוני אבטחה כל כך רחבים. יש לזה משמעות כבדה מבחינת עלויות. גם אם תהיה פריצה ללשכה, עדיין הנזק הוא למספר לקוחות מצומצם.

הממונה: אנו שואפים להגיע לנקודת האיזון: רמת סיכון סבירה בלי להעמיס רגולציה מיותרת. העברנו את ההוראה גם לגורמים מקצועיים בכדי לקבל חוות דעת, ביניהם KPMG, וכן כאמור קיבלנו הערות מהלשכות. בשלב הנוכחי אנחנו עדיין פתוחים להערות, ובכל מקום שנשתכנע שהעומס הרגולטורי מיותר, ניתן הקלות מסעיפי ההוראה לפי הצורך. מציין שכאשר ניהלנו את הדיאלוג מול הרשות הלאומית להגנת הסייבר הם העלו חשש להיווצרות מאגרי צל בלשכה, ופסלו את טיוטת ההוראה הראשונה. בעקבות זאת הערכנו מחדש את הסיכון והגענו למסקנה שהוא מתון, שכן הלשכות לא ישמרו את המידע ולכן לא יהיו מאגרי צל אבל עדיין קיים סיכון בזרימת המידע המזוהה דרך הלשכה.

חברת הוועדה: שתי בעלות הרישיון הנוכחיות עומדות ברגולציה דומה אבל הן שומרות רק מידע שלילי ויש להן מאגר יותר קטן. גם כיום הן מקבלות אלפי דוחות כל יום, ולכן יש פוטנציאל לנזק.

חבר הוועדה: חושב שזה לא נכון להמשיך ולחייב אותן ברגולציה כבדה ויש לתקן את הטעות שכן הדבר כרוך בעלויות כבדות, שבסופו של דבר יגולגלו על הלקוחות הפרטיים.

חברת הוועדה: אם רוצים שלשכות חדשות יכנסו לשוק, עלויות אבטחת המידע הכבדות יקשו עליהן.

חברת הוועדה: במאגר יש מידע על רוב האוכלוסייה והלשכה מתחברת למאגר. קיים סיכון שמישהו יתחבר למאגר דרך הלשכה בנקודת החולשה שלה. יחד עם זאת לשכות לא אמורות לפתח מאגרי צל שכן התפיסה שהן סולקות. צריך להיזהר לא להכביד על הלשכות, אבל קשה לבחון זאת מבלי לדעת מה העלויות של כל פרמטר בהוראה.

חבר הוועדה: מסכים שההוראה תחול על בנק ישראל אבל חושב שלשכה צריכה לקבל סט הנחיות אחר.

יו"ר הוועדה: מציע כי כשנעבור על סעיפי ההוראה הפרטניים, חברי הוועדה יציעו האם ניתן לצמצם וכיצד.

חברת הוועדה: מבקשת לקבל הסבר לסעיף 8 בהוראה לגבי ההקלות ללשכת אשראי שתפעל בסביבת אירוח של בנק ישראל.

הממונה: בעבר הייתה תפיסה שאנו נארח את מערכות הלשכה באופן מלא. במשך הזמן הגענו למסקנה שזה לא יפתור את סוגיית אבטחת המידע באופן מלא, שכן בסוף הלשכה תצטרך להוציא את המידע החוצה ללקוחות שלה. וכן, גם אם הלשכה תתארח, לא נרצה שייווצרו מאגרי צל עם מידע מזוהה, בעוד בנק ישראל שומר את המידע המזוהה בנפרד מהנתונים. על פני זמן גם גילינו שקיימת בעיה משפטית להכריח לשכה להתארח, לכן הצענו ללשכות לבחור בין מודל אירוח לבין מודל עצמאי. בסופו של התהליך הוחלט בשיתוף עם הלשכות כי הגישה למידע המזוהה תהיה במודל עצמאי והגישה למידע לא מזוהה תהיה במודל אירוח, כאשר הלשכות יוכלו להוציא החוצה רק תוצרים מוגדרים אגרגטיביים כגון נוסחת דירוג.

יו"ר הוועדה: עובר לסעיפים המתייחסים לדירקטוריון. האם לדירקטוריון צריכה להיות אחריות לדיווחים לממונה?

חברת הוועדה: חסר דיווח שנתי לממונה על תוצאות סקר הסיכונים ומבחני חדירה. חסרים גם דיווחים לממונה על תוצאות של דוחות ביקורת של הביקורת הפנימית.

הממונה: מה שחשוב הוא שהלשכה תבצע את סקר הסיכונים ומבחני חדירה. התפיסה הפיקוחית שלנו היא לא לקבל מראש את כל החומרים של הלשכה, אלא לממונה תהיה גמישות לקבל מהלשכה דיווחים ודוחות ביקורת בזמן אמת.

יו"ר הוועדה: מציע שתשקלו אם לבקש את סקר הסיכונים, או לחלופין תשקלו הגשה אלקטרונית שבה הלשכה מצהירה כי עשתה את הסקר בצירוף תמצית הממצאים בו או תצהיר תמציתי על עיקרי דוח הביקורת. בנוסף, מציע שהדירקטוריון יגדיר את סט הדיווחים לממונה, כאשר הדיווחים המפורטים בסעיף 27 בהוראה הם המינימום.

עובר לסעיפים המתייחסים לממונה על אבטחת מידע. האם ניתן להקל?

חברת הוועדה: צריך למנות ממונה על אבטחת מידע בהתאם לתקנות הגנת הפרטיות (אבטחת מידע).

חבר הוועדה: מציע שהממונה על אבטחת מידע יוכל למלא תפקיד נוסף ואולי אפילו מנהל טכנולוגיית המידע. בנוסף, עדיף שהוא יהיה עובד הלשכה ולא במיקור חוץ.

הממונה: החשיבה הייתה שבגופים קטנים בשל הצורך בידע מקצועי ייחודי עדיף שייקחו יועץ חיצוני.

חברת הוועדה: לדעתי חשיפות בסיכון גבוה צריכות להיות מטופלות בפרק זמן קצר יותר של 3 חודשים מביצוע הסקר במקום 6 חודשים (סעיף 24.6). גם תחקור אירועים והעברת המלצות צריך להיות מבוצע תוך חודש ולא תוך 3 חודשים (סעיף 24.7).

הממונה: החשש הוא שזה יגרום לכך שלשכות לא יסווגו חשיפות בסיכון גבוה. נשקול.

יו"ר הוועדה: עובר למסגרת העבודה לניהול הגנת המידע. חושב שהמילה "מסמך" בסעיפים 30.1 ו-30.2 מיותרת.

חבר הוועדה: לדעתי צריך לצמצם את מסגרת הגנת המידע בהוראה רק למערכות מידע לאשראי.

חברת הוועדה: לדעתי לא ניתן להפריד בין מערכות מידע לאשראי למערכות למידע נוסף.

הממונה: מציע לחדד את סעיף 6 בתחולה, שההוראה תחול על פעילות לשכה במתן שירותים לפי סעיפים 12 ו-13 לחוק נתוני אשראי, לרבות עיסוקים אשר הותרו לה לפי כללי נתוני אשראי.

חבר הוועדה: האם סעיף 42 הדורש שהלשכה תגדיר תכנית לביצוע הסקרים אצל ספקי מיקור חוץ לא מיותר, שכן אסור ללשכה להעביר מידע לספקי מיקור חוץ.

הממונה: הכוונה לדוגמא שאם ללשכה יש ספק שנותן לה שירות של אבטחת מידע, האחריות של הלשכה היא לפקח על הספק.

יו"ר הוועדה: קיימת הבחנה בין מתן הנחיות לביצוע הסקרים לבין וידוא של עמידה בסטנדרטים לגבי ספקי מיקור חוץ. מציע לכתוב שלשכה תוודא שספקי מיקור חוץ עומדים בסטנדרטים. עובר לבקרה וניטור - האם יש הערות?

חבר הוועדה: הדרישה בסעיף 46 של מערך לניטור מערכות מידע (SIEM) מטילה עלות כבדה על הלשכה שכן מדובר ברכיב מאוד יקר. מציע לאפשר ללשכה לרכוש זאת כשירות במקום לחייב אותה לרכוש את המערכת. מצטרף לחשש שאם ללשכות יהיו עלויות כבדות הם יגלגלו אותן על הלקוחות.

חברת הוועדה: מדובר במערכת חשובה שאוספת מקרים בנושא אבטחת מידע מכל מערכות המידע בארגון באמצעות חיישנים (אירועים חריגים, מתקפות וכד') ומדווחת עליהם למערכת מרכזית. מערכת הניטור חשובה כדי למנוע מצבים שבהם יגרם נזק לפרטיות הלקוחות.

יו"ר הוועדה: האם ניתן להקל, לדוגמא לפי היקף בקשות המידע שיהיו בלשכה, או ע"י דחיה של יישום הסעיף?

הממונה: נבדוק ונוסיף הבהרה שניתן גם לרכוש כשירות.

אנחנו קבענו את מחירי השירותים שיגבה המאגר מהלשכות בצו אגרות, ונפקח על המחירים שהלשכות יגבו מהלקוחות. אנו מקוים שנהיה בסביבה רגולטורית שיקבעו מחירים סבירים ויקומו לשכות, אחרת נשקול שוב את הרגולציה.

יו"ר הוועדה: עובר לקישוריות לרשת האינטרנט. למה לאפשר רשת אלחוטית לקבלת נתונים מהמאגר (סעיף 65)?

הממונה: נבדוק למה בדיוק התכוונו בסעיף.

חבר הוועדה: לגבי הפרדה בין סביבות ואבטחתן (סעיף 86), אם הסביבה שבה מנוהלים נתוני אשראי מופרדת, למה לא להחיל את ההוראה רק עליה?

חברת הוועדה: להערכתי זה לא יחסוך ללשכה עלויות.

הממונה: כאמור נחדד בתחולה של ההוראה כי אנו מתייחסים לפעילות של לשכת אשראי שתהיה תחת הרישיון שתקבל לפי החוק.

חבר הוועדה: לגבי ניהול הרשאות ובקרות גישה (סעיף 111), צריך לנסח כך שגישה מרחוק אסורה, והיא מותרת רק כפוף לדרישות שפורטו בסעיף. כל התקיפות באות מגישה מרחוק.

יו"ר הוועדה: אם נחמיר בסעיף זה, אולי נוכל להקל בסעיף של בקרה וניטור.

עובר לתכנית היערכות לניהול אירועי אבטחת מידע. לדעתי יש לחזק את הדרישות בחלק הזה של ההוראה. כשיש אירוע אבטחת מידע, דבר ראשון צריך לסגור את השירותים ל-24 שעות, עד שבודקים את הפריצה.

הממונה: מקבל את ההערה. מציע להוסיף לסעיף 115.2 את המילים: "לרבות הפסקת פעילות באופן זמני באירועים בחומרה גבוהה".

חבר הוועדה: סגירה של שירות מהסוג של חיווי אשראי יכולה להיות בעייתית ללקוחות, שכן הם לא יוכלו לבצע את הרכישות שלהם.

יו"ר הוועדה: עובר למיקור חוץ. למה צריך בהסכם התקשרות לקבלת שירותי מיקור חוץ להגדיר את רמת השירות (SLA)?

הממונה: ככל הנראה מדובר בסטנדרטים מינימליים במיקור חוץ. נבדוק.

יו"ר הוועדה: עובר לגיוס עובדים. מהן הדרישות בנושא מבנקים?

חברת הוועדה: בבנקים יש בדיקות מהימנות של עובדים.

חברת הוועדה: לגבי הדרכה, מציעה שגם בנק ישראל ישלח נציגים שלו ללשכות לתת הדרכות יזומות לעובדים, ולא להסתפק רק ברגולציה. יש יתרון בכך שעובדי הלשכה ישמעו על הנושא מהמקור - הרגולטור.

לגבי מסירת מידע באמצעים אלקטרוניים, בסעיף 179 - מבקש המידע יוכל לחזור בו מהסכמתו בכל עת, מציעה להוסיף את המילים "לפני מסירת הדוח".

חברת הוועדה: לגבי התיעוד, מציעה לסדר את הסעיפים בהוראה כך שתהיה הבחנה בין מה ניתן לשמור ומה לא ניתן לשמור.

יו"ר הוועדה: אם תובעים לשכה, איך היא יכולה לקבל את נתוני המקור.

נציגת המחלקה המשפטית: כפי שצוין אגב שאלת שמירת המידע על ידי הלשכות, הלשכה תוכל לקבל את הנתונים מהמאגר של בנק ישראל אם הם דרושים לה לצורך הליך משפטי, בהתאם לסעיף 23(ב)(1) לחוק.

יו"ר הוועדה: מה קורה אם יש טעות בנתונים?

חברת הוועדה: האחריות להעברת נתונים תקינים היא לא של הלשכה ולא של בנק ישראל, אלא של מקור המידע.

נציגת המחלקה המשפטית: לבנק ישראל יש אחריות להעביר את הנתונים המקוריים. אם לקוח חושב שיש טעות בנתונים, הוא יכול לפנות לבנק ישראל, ובנק ישראל יערוך בירור עם מקור המידע.

המלצה:

להכניס תיקונים בהוראת ניהול המידע והגנתו ללשכות, לפי הערות חברי הוועדה, כמפורט בדיון.